

Department of Energy

Pt. 1016

date the loan was presented to DOE for payment or re-insurance.

(b) The DOJ has exclusive jurisdiction over the debts referred to it pursuant to this section. DOE shall refrain from having any contact with the debtor and shall direct all debtor inquiries concerning the claim to the DOJ. DOE shall notify the DOJ immediately of any payments credited by DOE to the debtor's account after referral of a debt or claim under this section. The DOJ shall notify DOE, in a timely manner, of any payments it receives from the debtor.

§ 1015.503 Claims Collection Litigation Report.

(a) Unless excepted by the DOJ, DOE shall complete the CCLR (see § 1015.301 of this part), accompanied by a signed Certificate of Indebtedness, to refer all administratively uncollectible claims to the DOJ for litigation. DOE shall complete all of the sections of the CCLR appropriate to each claim as required by the CCLR instructions and furnish such other information as may be required in specific cases.

(b) DOE shall indicate clearly on the CCLR the actions it wishes the DOJ to take with respect to the referred claim. The CCLR permits DOE to indicate specifically any of a number of litigative activities which the DOJ may pursue, including enforced collection, judgment lien only, renew judgment lien only, renew judgment lien and enforce collection, program enforcement, foreclosure only, and foreclosure and deficiency judgment.

(c) DOE also shall use the CCLR to refer claims to the DOJ to obtain the DOJ's approval of any proposals to compromise the claims or to suspend or terminate DOE collection activity.

§ 1015.504 Preservation of evidence.

DOE will take care to preserve all files and records that may be needed by the DOJ to prove its claims in court. DOE ordinarily will include certified copies of the documents that form the basis for the claim in the packages referring its claims to the DOJ for litigation. DOE shall provide originals of such documents immediately upon request by the DOJ.

§ 1015.505 Minimum amount of referrals to the Department of Justice.

(a) DOE shall not refer for litigation claims of less than \$2,500, exclusive of interest, penalties, and administrative costs, or such other amount as the Attorney General shall from time to time prescribe. The DOJ promptly shall notify DOE if the Attorney General changes this minimum amount.

(b) DOE shall not refer claims of less than the minimum amount unless:

(1) Litigation to collect such smaller claims is important to ensure compliance with DOE's policies or programs;

(2) The claim is being referred solely for the purpose of securing a judgment against the debtor, which will be filed as a lien against the debtor's property pursuant to 28 U.S.C. 3201 and returned to DOE for enforcement; or

(3) The debtor has the clear ability to pay the claim and the Government effectively can enforce payment, with due regard for the exemptions available to the debtor under state and Federal law and the judicial remedies available to the Government.

(4) DOE will consult with the Financial Litigation Staff of the Executive Office for United States Attorneys in the DOJ prior to referring claims valued at less than the minimum amount.

PART 1016—SAFEGUARDING OF RESTRICTED DATA

GENERAL PROVISIONS

Sec.

1016.1 Purpose.

1016.2 Scope.

1016.3 Definitions.

1016.4 Communications.

1016.5 Submission of procedures by access permit holder.

1016.6 Specific waivers.

1016.7 Interpretations.

PHYSICAL SECURITY

1016.8 Approval for processing access permittees for security facility approval.

1016.9 Processing security facility approval.

1016.10 Grant, denial, or suspension of security facility approval.

1016.11 Cancellation of requests for security facility approval.

1016.12 Termination of security facility approval.

1016.21 Protection of Restricted Data in storage.

1016.22 Protection while in use.

§ 1016.1

10 CFR Ch. X (1–1–08 Edition)

- 1016.23 Establishment of security areas.
- 1016.24 Special handling of classified material.
- 1016.25 Protective personnel.

CONTROL OF INFORMATION

- 1016.31 Access to Restricted Data.
- 1016.32 Classification and preparation of documents.
- 1016.33 External transmission of documents and material.
- 1016.34 Accountability for Secret Restricted Data.
- 1016.35 Authority to reproduce Restricted Data.
- 1016.36 Changes in classification.
- 1016.37 Destruction of documents or material containing Restricted Data.
- 1016.38 Suspension or revocation of access authorization.
- 1016.39 Termination, suspension, or revocation of security facility approval.
- 1016.40 Termination of employment or change of duties.
- 1016.41 Continued applicability of the regulations in this part.
- 1016.42 Reports.
- 1016.43 Inspections.
- 1016.44 Violations.

AUTHORITY: Sec. 161i of the Atomic Energy Act of 1954, 68 Stat. 948 (42 U.S.C. 2201).

SOURCE: 48 FR 36432, Aug. 10, 1983, unless otherwise noted.

GENERAL PROVISIONS

§ 1016.1 Purpose.

The regulations in this part establish requirements for the safeguarding of Secret and Confidential Restricted Data received or developed under an access permit. This part does not apply to Top Secret information since no such information may be forwarded to an access permittee within the scope of this regulation.

§ 1016.2 Scope.

The regulations in this part apply to all persons who may require access to Restricted Data used, processed, stored, reproduced, transmitted, or handled in connection with an access permit.

§ 1016.3 Definitions.

(a) *Access authorization or security clearance.* An administrative determination by the DOE that an individual who is either a DOE employee, applicant for employment, consultant, assignee, other Federal department or agency employee (and other persons

who may be designated by the Secretary of Energy), or a DOE contractor or subcontractor employee and an access permittee is eligible for access to Restricted Data. Access authorizations or security clearances granted by DOE are designated as “Q,” “Q(X),” “L,” “L(X),” “Top Secret,” or “Secret.” For the purpose of this chapter only “Q,” “Q(X),” “L,” and “L(X)” access authorizations or clearances will be defined.

(1) “Q” access authorizations or clearances are based upon full field investigations conducted by the Federal Bureau of Investigation, Office of Personnel Management, or another Government agency which conducts personnel security investigations. They permit an individual to have access, on a “need to know” basis, to Top Secret, Secret, and Confidential Restricted Data, Formerly Restricted Data, National Security Information, or special nuclear material in Category I or II quantities as required in the performance of duties.

(2) “Q(X)” access authorizations or clearances are based upon the same full field investigations as described in §1016.3(a)(1), above. When “Q” access authorizations or clearances are granted to access permittees they are identified as “Q(X)” access authorizations or clearances and authorize access only to the type of Secret Restricted Data as specified in the permit and consistent with appendix A, 10 CFR part 725, “Categories of Restricted Data Available.”

(3) “L” access authorizations or clearances are based upon National Agency Checks and Inquiries (NACI) for Federal employees, or National Agency Checks (NAC) for non-Federal employees, conducted by the Office of Personnel Management. They permit an individual to have access, on a “need to know” basis, to Confidential Restricted Data, Secret and Confidential Formerly Restricted Data, or Secret and Confidential National Security Information, required in the performance of duties, provided such information is not designated “CRYPTO” (classified cryptographic information), other classified communications security (“COMSEC”) information, or intelligence information.

Department of Energy

§ 1016.3

(4) “L(X)” access authorizations or clearances are based upon the same National Agency Checks as described in paragraph (a)(3), of this section. When “L” access authorizations or clearances are granted to access permittees, they are identified as “L(X)” access authorizations or clearances and authorize access only to the type of Confidential Restricted Data as specified in the permit and consistent with appendix A, 10 CFR part 725, “Categories of Restricted Data Available.”

(b) *Act.* The Atomic Energy Act of 1954 (68 Stat. 919) as amended.

(c) *Authorized classifier.* An individual authorized in writing by appropriate DOE authority to classify, declassify, or downgrade the classification of information, work, projects, documents, and materials.

(d) *Classified mail address.* A mail address established for each access permittee approved by the DOE to which all Restricted Data for the permittee is to be sent.

(e) *Classified matter.* Documents and material containing classified information.

(f) *Combination lock.* A built-in combination lock on a security container which is of tempered steel alloy hard plate, at least ¼” in thickness and Rockwell hardness of C-63 to C-65, of sufficient size and so located as to sufficiently impede access to the locking mechanism by drilling of the lock or container.

(g) *DOE.* The United States Department of Energy or its duly authorized representatives.

(h) *Document.* Any piece of recorded information regardless of its physical form or characteristics.

(i) *Formerly Restricted Data.* Classified information jointly determined by the DOE and the Department of Defense to be related primarily to the military utilization of atomic weapons and removed by the DOE from the Restricted Data category pursuant to section 142(d) of the Atomic Energy Act of 1954, as amended.

(j) *Infraction.* An act or omission involving failure to comply with DOE safeguards and security orders or directives, and may include a violation of law.

(k) *Intrusion alarm.* A tamper-indicating electrical, electro-mechanical, electro-optical, electronic or similar device which will detect unauthorized intrusion by an individual into a building or security area, and alert protective personnel by means of actuated visible and audible signals.

(l) *Material.* A chemical substance without regard to form; fabricated or processed item; or assembly, machinery, or equipment.

(m) *Matter.* Documents or material.

(n) *National Security.* The national defense and foreign relations of the United States.

(o) *National Security Information.* Information that has been determined pursuant to Executive Order 12958, as amended “Classified National Security Information” and Executive Order 13292 “Further Amendment to Executive Order 12958, as Amended, Classified National Security Information” or any predecessor order to require protection against unauthorized disclosure and that is so designated.

(p) *“Need to know.”* A determination by persons having responsibility for classified information or matter, that a proposed recipient’s access to such classified information or matter is necessary in the performance of official, contractual, or access permit duties of employment under cognizance of the DOE.

(q) *Permittee.* The holder of an Access Permit issued pursuant to the regulations set forth in 10 CFR part 725, “Permits For Access to Restricted Data.”

(r) *Person.* Any individual, corporation, partnership, firm, association, trust, estate, public or private institution, group, Government agency other than DOE, any State or any political subdivision of, or any political entity within a State, or other entity; and any legal successor, representative, agency, or agency of the foregoing.

(s) *Protective personnel.* Guards or watchmen or other persons designated responsibility for the protection of classified matter.

(t) *Restricted Data.* All data concerning design, manufacture, or utilization of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the

§ 1016.4

production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to section 142 of the Act.

(u) *Security area*. A physically defined space containing classified matter and subject to physical protection and personnel access controls.

(v) *Security clearance*. See access authorization.

(w) *Security facility*. Any facility, including an access permittee, which has been approved by the DOE for using, processing, storing, reproducing, transmitting, or handling classified matter.

(x) *Security facility approval*. A determination by the DOE that a facility, including an access permittee, is eligible to use, process, store, reproduce, transmit, or handle classified matter.

(y) *Security Plan*. A written plan by the access permittee, and submitted to the DOE for approval, which outlines the permittee's proposed security procedures and controls for the protection of Restricted Data and which includes a floor plan of the area in which the matter is to be used, processed, stored, reproduced, transmitted, or handled.

(z) *Security survey*. An onsite examination by a DOE representative of all devices, equipment, and procedures employed at a security facility to safeguard classified matter.

[48 FR 36432, Aug. 10, 1983, as amended at 71 FR 68735, Nov. 28, 2006]

§ 1016.4 Communications.

Communications concerning rule-making, i.e., petition to change part 1016, should be addressed to the Chief Health, Safety and Security Officer, HS-1/Forrestal Building, Office of Health, Safety and Security, U.S. Department of Energy, 1000 Independence Avenue, SW., Washington, DC 20585. All other communications concerning the regulations in this part should be addressed to the cognizant DOE or National Nuclear Security Administration (NNSA) office.

[71 FR 68735, Nov. 28, 2006]

§ 1016.5 Submission of procedures by access permit holder.

No access permit holder shall have access to Restricted Data until he shall have submitted to the DOE a written

10 CFR Ch. X (1-1-08 Edition)

statement of his procedures for the safeguarding of Restricted Data and for the security education of his employees, and DOE shall have determined and informed the permittee that his procedures for the safeguarding of Restricted Data are in compliance with the regulations in this part and that his procedures for the security education of his employees, who will have access to Restricted Data, are informed about and understand the regulations in this part.

§ 1016.6 Specific waivers.

DOE may, upon application of any interested party, grant such waivers from the requirements of this part as it determines are authorized by law and will not constitute an undue risk to the common defense and security.

§ 1016.7 Interpretations.

Except as specifically authorized by the Secretary of Energy in writing, no interpretation of the meaning of the regulations in this part by any officer or employee of DOE other than a written interpretation by the General Counsel will be recognized to be binding upon DOE.

PHYSICAL SECURITY

§ 1016.8 Approval for processing access permittees for security facility approval.

(a) An access permittee who has a need to use, process, store, reproduce, transmit, or handle Restricted Data at any location in connection with its permit shall promptly request a DOE security facility approval.

(b) The request shall include the following information: The name and address of the permittee; the extent and scope of the classified activity and the highest classification of Restricted Data to be received; a written statement in the form of a security plan which outlines the permittee's proposed security procedures and controls for the protection of Restricted Data, including a floor plan of the areas(s) in which the classified matter is to be used, processed, stored, reproduced, transmitted, and handled.

(c) The DOE will promptly inform the permittee of the acceptability of the

Department of Energy

§ 1016.22

request for further processing and will notify the permittee of its decision in writing.

§ 1016.9 Processing security facility approval.

The following receipt of an acceptable request for security facility approval, the DOE will perform an initial security survey of the permittee's facility to determine that granting a security facility approval would be consistent with the national security. If DOE makes such a determination, security facility approval will be granted. If not, security facility approval will be withheld pending compliance with the security survey recommendations or until a waiver is granted pursuant to § 1016.6 of this part.

§ 1016.10 Grant, denial, or suspension of security facility approval.

Notification of the DOE's grant, denial, or suspension of security facility approval will be furnished the permittee in writing, or orally with written confirmation. This information may also be furnished to representatives of the DOE, DOE contractors, or other Federal agencies having a need to transmit Restricted Data to the permittee.

§ 1016.11 Cancellation of requests for security facility approval.

When a request for security facility approval is to be withdrawn or cancelled, the DOE Operations Office will be notified by the requester immediately by telephone and confirmed in writing so that processing of this approval may be terminated.

§ 1016.12 Termination of security facility approval.

Security facility approval will be terminated when:

(a) There is no longer a need to use, process, store, reproduce, transmit, or handle Restricted Data at the facility; or

(b) The DOE makes a determination that continued security facility approval is not in the interest of national security.

In such cases the permittee will be notified in writing of the determination,

and the procedures outlined in § 1016.39 of this part will apply.

§ 1016.21 Protection of Restricted Data in storage.

(a) Persons who possess Restricted Data pursuant to an Access Permit shall store Secret and Confidential documents and material when not in use in accordance with one of the following methods:

(1) In a locked vault, safe, or safe-type steel file cabinet having a 3-position dial-type combination lock; or

(2) In a dual key, bank safety deposit box; or

(3) In a steel file cabinet secured by a steel lock bar and a 3-position dial-type changeable combination padlock; or

(4) In a locked steel file cabinet when located in a security area established under § 1016.23 or when the cabinet or the place in which the cabinet is located is under DOE-approved intrusion alarm protection.

(b) Changes of combination: Each permittee shall change the combination on locks of his safekeeping equipment whenever such equipment is placed in use, whenever an individual knowing the combination no longer requires access to the repository as a result of change in duties or position in the permittee's organization, or termination of employment with the permittee or whenever the combination has been subjected to compromise, and in any event at least once a year. Permittees shall classify records of combinations no lower than the highest classification of the documents and material authorized for storage in the safekeeping equipment concerned.

(c) The lock on safekeeping equipment of the type specified in paragraph (a)(4) of this section shall be replaced immediately whenever a key is lost.

§ 1016.22 Protection while in use.

While in use, documents and material containing Restricted Data shall be under the direct control of an appropriately cleared individual, and the Restricted Data shall be capable of being removed from sight immediately.

§ 1016.23

§ 1016.23 Establishment of security areas.

(a) When, because of their nature or size, it is impracticable to safeguard documents and material containing Restricted Data in accordance with the provisions of §§ 1016.21 and 1016.22, a security area to protect such documents and material shall be established.

(b) The following controls shall apply to security areas:

(1) Security areas shall be separated from adjacent areas by a physical barrier designed to prevent entrance into such areas, and access to the Restricted Data within the areas, by unauthorized individuals.

(2) During working hours, admittance shall be controlled by an appropriately cleared individual posted at each unlocked entrance.

(3) During nonworking hours, admittance shall be controlled by protective personnel on patrol, with protective personnel posted at unlocked entrances, or by such intrusion alarm system as DOE may approve.

(4) Each individual authorized to enter a security area shall be issued a distinctive badge or pass when the number of employees assigned to the area exceeds thirty.

§ 1016.24 Special handling of classified material.

When the Restricted Data contained in material is not ascertainable by observation or examination at the place where the material is located and when the material is not readily removable because of size, weight, radioactivity, or similar factors, DOE may authorize the permittee to provide such lesser protection than is otherwise required by §§ 1016.21 to 1016.23 inclusive, as DOE determines to be commensurate with the difficulty of removing the material.

§ 1016.25 Protective personnel.

Whenever protective personnel are required by § 1016.23, such protective personnel shall:

(a) Possess a “Q” or “L” security clearance or access authorization or “Q(X)” or “L(X)” access authorization if the Restricted Data being protected is classified Confidential, or a “Q” security clearance or access authoriza-

10 CFR Ch. X (1–1–08 Edition)

tion or “Q(X)” access authorization if the Restricted Data being protected is classified Secret.

(b) Be armed with sidearms of not less than .38 caliber.

CONTROL OF INFORMATION

§ 1016.31 Access to Restricted Data.

(a) Except as DOE may authorize, no person subject to the regulations in this part shall permit any individual to have access to Secret or Confidential Restricted Data in his possession unless the individual has an appropriate security clearance or access authorization granted by DOE, or has been certified by DOD or NASA through DOE, and:

(1) The individual is authorized by an Access Permit to receive Restricted Data in the categories involved and, in the case of Secret Restricted Data, the permittee determines that such access is required in the course of his duties, or

(2) The individual needs such access in connection with such duties as a DOE employee or DOE contractor employee, or as certified by DOD or NASA.

(b) Inquiries concerning the clearance status of individuals, the scope of Access Permits, or the nature of contracts should be addressed to the cognizant DOE or NNSA office.

[48 FR 36432, Aug. 10, 1983, as amended at 71 FR 68735, Nov. 28, 2006]

§ 1016.32 Classification and preparation of documents.

(a) *Classification.* Restricted Data generated or possessed by an Access Permit holder must be appropriately marked. CG-UF-3, “Guide to the Unclassified Fields of Research,” will be furnished each permittee. In the event a permittee originates classified information which falls within the definition of Restricted Data or information which he is not positive is not within that definition and CG-UF-3 does not provide positive classification guidance for such information, he shall designate the information as Confidential, Restricted Data and request classification guidance from the DOE through the Classification Officer at the cognizant DOE or NNSA office, who will

Department of Energy

§ 1016.33

refer the request to the Director, Office of Classification, HS-90/Germantown Building, Office of Health, Safety and Security, U.S. Department of Energy, 1000 Independence Avenue, SW., Washington, DC 20585-1290 if he does not have authority to provide the guidance.

(b) *Classification consistent with content.* Each document containing Restricted Data shall be classified Secret or Confidential according to its own content.

(c) *Document which custodian believes improperly classified or lacking appropriate classification markings.* If a person receives a document which, in his opinion, is not properly classified, or omits the appropriate classification markings, he shall communicate with the sender and suggest the classification which he believes appropriate. Pending final determination of proper classification, such documents shall be safeguarded with the highest classification in question.

(d) *Classification markings.* Unless otherwise authorized below, the assigned classification of a document shall be conspicuously marked or stamped at the top and bottom of each page and on the front cover, if any, and the document shall bear the following additional markings on the first page and on the front cover:

RESTRICTED DATA

This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Its transmittal or the disclosure of its contents in any manner to an unauthorized person is prohibited.

(e) *Documentation.* (1) All Secret documents shall bear on the first page a properly completed documentation stamp such as the following: This document consists of __ pages. Copy No. __ of __ Series __.

(2) The series designation shall be a capital letter beginning with the letter "A" designating the original set of copies prepared. Each subsequent set of copies of the same documents shall be identified by the succeeding letter of the alphabet.

(f) *Letter of transmittal.* A letter of transmitting Restricted Data shall be marked with a classification at least as high as its highest classified enclosure.

When the contents of the letter of transmittal warrant lower classification or requires no classification, a stamp or marking such as the following shall be used in the letter:

When separated from enclosures handle this document as ____.

(g) *Permanently fastened documents.* Classified books or pamphlets, the pages of which are permanently and securely fastened together, shall be conspicuously marked or stamped with the assigned classification in letters at least one-fourth (1/4) inch in height at the top and bottom on the outside front cover, on the title page, on the front page, and on the inside and outside of the back cover. The additional markings referred to in paragraph (d) of this section shall be placed on the first page and on the front cover.

(h) *Physically connected documents.* The classification of a file or group of physically connected documents shall be at least as high as that of the most highly classified document therein. It shall bear only one overall classification, although pages, paragraphs, sections, or components thereof may bear different classifications. Each document separated from the file or group shall be handled in accordance with its individual classification.

(i) *Attachment of security markings.* Documents which do not lend themselves to marking or stamping shall have securely affixed or attached a tag, sticker, or similar device bearing the appropriate security markings.

[48 FR 36432, Aug. 10, 1983, as amended at 71 FR 68735, Nov. 28, 2006]

§ 1016.33 External transmission of documents and material.

(a) *Restrictions.* (1) Documents and material containing Restricted Data shall be transmitted only to persons who possess appropriate clearance or access authorization and are otherwise eligible for access under the requirements of § 1016.31.

(2) In addition, such documents and material shall be transmitted only to persons who possess facilities for their physical security consistent with this part. Any person subject to the regulations in this part who transmits such documents or material shall be deemed to have fulfilled his obligations under

§ 1016.34

10 CFR Ch. X (1–1–08 Edition)

this subparagraph by securing a written certification from the prospective recipient that such recipient possesses facilities for its physical security consistent with this part.

(3) Documents and material containing Restricted Data shall not be exported from the United States without prior authorization of DOE.

(b) *Preparation of documents.* Documents containing Restricted Data shall be prepared for transmission outside an individual installation in accordance with the following:

(1) They shall be enclosed in two sealed, opaque envelopes or wrappers.

(2) The inner envelope or wrapper shall be addressed in the ordinary manner and sealed with tape, the appropriate classification shall be placed on both sides of the envelope, and the additional marking referred to in § 1016.32(d) shall be placed on the side bearing the address.

(3) The outer envelope or wrapper shall be addressed in the ordinary manner. No classification, additional marking, or other notation shall be affixed which indicates that the document enclosed therein contains classified information or Restricted Data.

(4) A receipt which identifies the document, the date of transfer, the recipient, and the person transferring the document shall accompany the document and shall be signed by the recipient and returned to the sender whenever the custody of a Secret document is transferred.

(c) *Preparation of material.* Material, other than documents, containing Restricted Data shall be prepared for shipment outside an individual installation in accordance with the following:

(1) The material shall be so packaged that the classified characteristics will not be revealed.

(2) A receipt which identifies the material, the date of shipment, the recipient, and the person transferring the material shall accompany the material, and the recipient shall sign such receipt whenever the custody of Secret material is transferred.

(d) *Methods of transportation.* (1) Secret matter shall be transported only by one of the following methods:

(i) By messenger-courier system specifically created for that purpose.

(ii) Registered mail.

(iii) By protective services provided by United States air or surface commercial carriers under such conditions as may be preserved by the DOE.

(iv) Individuals possessing appropriate DOE security clearance or access authorization who have been given written authority by their employers.

(2) Confidential matter may be transported by one of the methods set forth in paragraph (d)(1) of this section or by U.S. first class, express, or certified mail.

(e) *Telecommunication of classified information.* There shall be no telecommunication of Restricted Data unless the secure telecommunication system has been approved by the DOE.

(f) *Telephone conversations.* Classified information shall not be discussed over the telephone.

§ 1016.34 Accountability for Secret Restricted Data.

Each permittee possessing documents containing Secret Restricted Data shall establish a document accountability procedure and shall maintain records to show the disposition of all such documents which have been in his custody at any time.

§ 1016.35 Authority to reproduce Restricted Data.

Secret Restricted Data will not be reproduced without the written permission of the originator, his successor, or high authority. Confidential Restricted Data may be reproduced to the minimum extent necessary consistent with efficient operation without the necessity for permission.

§ 1016.36 Changes in classification.

Documents containing Restricted Data shall not be downgraded or declassified except as authorized by DOE. Requests for downgrading or declassification shall be submitted to the cognizant DOE or NNSA office or Office of Classification, HS-90/Germantown Building, U.S. Department of Energy, 1000 Independence Avenue, SW., Washington, DC 20585-1290. If the appropriate authority approves a change of classification or declassification, the

Department of Energy

§ 1016.42

previous classification marking shall be canceled and the following statement, properly completed, shall be placed on the first page of the document:

Classification canceled (or changed to)

(Insert appropriate classification)

by

(Person authorizing change in classification)
by

(Signature of person making change and date thereof)

Any persons making a change in classification or receiving notice of such a change shall forward notice of the change in classification to holders of all copies as shown in their records.

[48 FR 36432, Aug. 10, 1983, as amended at 71 FR 68735, Nov. 28, 2006]

§ 1016.37 Destruction of documents or material containing Restricted Data.

Documents containing Restricted Data may be destroyed by burning, pulping, or another method that assures complete destruction of the information which they contain. If the document contains Secret Restricted Data, a permanent record of the subject, title, report number of the document, its date of preparation, its series designation and copy number, and the date of destruction shall be signed by the person destroying the document and shall be maintained in the office of the last custodian. Restricted Data contained in material, other than documents, may be destroyed only by a method that assures complete obliteration, removal, or destruction of the Restricted Data.

§ 1016.38 Suspension or revocation of access authorization.

In any case where the access authorization of an individual subject to the regulations in this part is suspended or revoked in accordance with the procedures set forth in 10 CFR part 710, such individual shall, upon due notice from DOE of such suspension or revocation and demand by DOE, deliver to DOE any and all Restricted Data in his possession for safekeeping and such further disposition as DOE determines to be just and proper.

§ 1016.39 Termination, suspension, or revocation of security facility approval.

(a) If the need to use, process, store, reproduce, transmit, or handle classified matter no longer exists, the security facility approval will be terminated. The permittee may deliver all Restricted Data to the DOE or to a person authorized to receive them; or the permittee may destroy all such Restricted Data. In either case, the facility must submit a certification of nonpossession of Restricted Data to the DOE.

(b) In any instance where security facility approval has been suspended or revoked based on a determination of the DOE that further possession of classified matter by the permittee would endanger the common defense and national security, the permittee shall, upon notice from the DOE, immediately deliver all Restricted Data to the DOE along with a certificate of nonpossession of Restricted Data.

§ 1016.40 Termination of employment or change of duties.

Each permittee shall furnish promptly to DOE written notification of the termination of employment of each individual who possesses an access authorization under his Permit or whose duties are changed so that access to Restricted Data is no longer needed. Upon such notification, DOE may:

(a) Terminate the individual's access authorization, or

(b) Transfer the individual's access authorization to the new employer of the individual to allow continued access to Restricted Data where authorized, pursuant to DOE regulations.

§ 1016.41 Continued applicability of the regulations in this part.

The expiration, suspension, revocation, or other termination of a security clearance or access authorization or security facility approval shall not relieve any person from compliance with the regulations in this part.

§ 1016.42 Reports.

Each permittee shall immediately report to the DOE office administering the permit any alleged or suspected violation of the Atomic Energy Act of

§ 1016.43

1954, as amended, Espionage Act, or other Federal statutes related to Restricted Data. Additionally, the permittee shall report any infractions, losses, compromises, or possible compromise of Restricted Data.

§ 1016.43 Inspections.

The DOE shall make such inspections and surveys of the premises, activities, records, and procedures of any person subject to the regulations in this part as DOE deems necessary to effectuate the purposes of the Act, Executive Order 12958, as amended, and DOE orders and procedures.

[48 FR 36432, Aug. 10, 1983, as amended at 71 FR 68735, Nov. 28, 2006]

§ 1016.44 Violations.

An injunction or other court order may be obtained prohibiting any violation of any provision of the Act or any regulation or order issued thereunder. Any person who willfully violates, attempts to violate, or conspires to violate any provision of the Act or any regulation or order issued thereunder, including the provisions of this part, may be guilty of a crime and upon conviction may be punished by fine or imprisonment, or both, as provided by law.

PART 1017—IDENTIFICATION AND PROTECTION OF UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION

Sec.

1017.1 Purpose and scope.

1017.2 Applicability.

1017.3 Definitions.

1017.4 Policy.

1017.5 Prohibitions.

1017.6 Exemptions.

1017.7 Identification of unclassified controlled nuclear information.

1017.8 Categories of unclassified controlled nuclear information.

1017.9 Adverse effect test.

1017.10 Nuclear material determinations.

1017.11 Quarterly report.

1017.12 Review and denial of documents or material.

1017.13 Retirement of documents or material.

1017.14 Joint information, documents, or material.

1017.15 Markings on documents or material.

10 CFR Ch. X (1–1–08 Edition)

1017.16 Access to unclassified controlled nuclear information.

1017.17 Physical protection requirements.

1017.18 Violations.

AUTHORITY: 42 U.S.C. 2168; 28 U.S.C. 2461 note.

SOURCE: 50 FR 15822, Apr. 22, 1985, unless otherwise noted.

§ 1017.1 Purpose and scope.

(a) This part contains regulations of the Department of Energy (DOE) implementing section 148 (42 U.S.C. 2168) of the Atomic Energy Act which prohibits the unauthorized dissemination of certain unclassified government information. This information, identified by the term “Unclassified Controlled Nuclear Information” (UCNI), is limited to information concerning atomic energy defense programs.

(b) These regulations—

(1) Provide for the review of information prior to its designation as UCNI;

(2) Describe how information is determined to be UCNI;

(3) Establish minimum physical protection standards for documents and material containing UCNI;

(4) Specify who may have access to UCNI; and

(5) Establish a procedure for the imposition of penalties on persons who violate section 148 of the Atomic Energy Act or any regulation or order of the Secretary issued under section 148 of the Atomic Energy Act, including these regulations.

§ 1017.2 Applicability.

These regulations apply to—

(a) Any person authorized access to UCNI;

(b) Any person not authorized access to UCNI who acquires, attempts to acquire, or conspires to acquire, in violation of these regulations, Government information in any document or material containing an UCNI notice (refer to § 1017.15); and

(c) Any person not authorized access to UCNI but who wants to be authorized access to UCNI.

§ 1017.3 Definitions.

As used in this part—

(a) *Atomic Energy Act* means the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 *et seq.*).